Innovative uses as a result of DNSSEC

Jay Daley .nz

p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited

Disclaimer

- This is highly opinionated
- I may be wrong

Spreading usage

- ADDRESS MAPPING – where do I connect?
- SECURITY – how do I connect?
  - Current RRs (e.g. SSHFP) unused
  - DANE will change this
- POLICY – should I connect?
  - Growth area
  - Squeeze policy into one line! - madness

Bifurcation

- Useful generic characteristics of DNS
  - By design: Scalable, distributed, route around failure, compact, replicating, SECURE
  - By accident: Firewall transparent, high investment
- So seems natural for databases
  - More clever database features needed
    - Pointers, indexes etc
  - But - loose synchronisation under threat

Peer 2 Peer DNS

- Threat from asymmetry of attack bandwidth vs defense bandwidth - DDoS
- P2P natural mitigation
- P2P is all about trust
- DNSSEC provides trust for data integrity
- BUT still no trust for server integrity
  - Not hard to solve!
- AND high performance not trivial

Side effects

- Crypto in Enterprise now common
- DNSSEC another crypto function
  - Good examples of management processes
    - e.g. Split of KSK, ZSK
- Clear now – Enterprises need CA function
  - Following that best practice
    - Organisational root keys
    - Translate keys between different formats (hard)

Any questions?

jay@nzrs.net.nz

p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED